Identity Management for Electronic Negotiations

Omid Tafreschi[1]*, Janina Fengel[2] and Michael Rebstock[2]

[1] Darmstadt University of Technology
Dolivostr. 15, 64293 Darmstadt, Germany

[2] Darmstadt University of Applied Sciences
Haardtring 100, 64295 Darmstadt, Germany

Abstract. Using the Internet as the medium for transporting sensitive business data poses risks to companies. Before conducting business electronically, a company should take preventive measures against data manipulations and possible data misuse. One initial step could be obtaining certainty about the true identity of a potential business partner responding to a request or tender. In this paper we report on the development of a concept for identity management to introduce trust for electronic negotiations.
We describe the character of electronic negotiations and give an example for a possible use-case scenario of our concept. For this we choose the most complex type of negotiations in the business domain, which are interactive bilateral multiattributive negotiations. Based on a general application architecture for such negotiations developed in a research project, we show the necessity of security provisions and introduce a security concept for identity management. We argue that the development of authentication and authorization services for the identity management of business partners involved in a negotiation are not only crucial but also an enhancement for electronic marketplaces.

1 Introduction

Electronic negotiations are of increasing importance in today's e-business applications, especially since integration is becoming a major consideration in the forming of business processes. For achieving effective procurement and supply chain management, seamless integration in processing complex transactions is required [1]. Supply chain decisions within in organizations depend on the results of negotiations with the potential partners of a transaction. Supporting these negotiations electronically, and supplying their integration with internal applications, allows major progress in internal and external business process integration as well as decision support and the facilitation of supply chain management.
Consequently the nature of electronic negotiation applications has become strongly inter-organizational. Negotiations and contracts form the economic links between organizations as elements of the information chain emerging during the process. Next

* The author was supported by the German Federal Ministry of Education and Research under grant 01AK706C, project *Premium*.

Tafreschi O., Fengel J. and Rebstock M. (2005).
Identity Management for Electronic Negotiations.
In *Proceedings of the 2nd International Workshop on Computer Supported Activity Coordination*, pages 38-47
DOI: 10.5220/0002562600380047

to research-oriented aspects business application requirements have become relevant. The interface nature of electronic negotiations implies social and legal, but also organizational (business processes and documents) and technical (application integration) aspects [2]. Research and application development has already been done in this area, often focusing on auctions and tenders. But whereas in the 1990s electronic negotiations have largely been a domain of stand-alone applications, today, also with focus on EDI and supply chain transactions, their inter-organizational aspects become prevailing [3–6].

True integration between organizations and their applications requires seamless electronic data exchange in order to enable the exploitation of process optimization and the resulting competitive advantages. But due to the inter-organizational character of electronic negotiations in the business domain combined with the use of the Internet, organizations are becoming more exposed to malicious acts than in pre-electronic times. Consequently, a simple adoption of negotiation processes to the Internet is subject to manipulation and data misuse. Numerous security issues can arise. Addressing these issues is prerequisite for electronic negotiations. In this paper we focus on one specific security service, which is identity management.

In section 2 we explain the concept of electronic negotiations focusing on the B2B domain. A negotiation may be conducted in form of an auction, tender, exchange or bilateral considering either one or several attributes at the same time. As an example of the most complex type of negotiations we describe interactive bilateral multiattributive negotiations, as those are the most common [7]. We then discuss an application architecture for this type of negotiations and introduce and analyze the main security aspects within this context, concentrating on identity management. Based on our analysis, we develop a concept for this security service. It provides authentication of the business partners involved in a negotiation and access control through authorization. Furthermore, we show how security related information can also be used to support the implementation of business policies. We conclude with related work.

2 Electronic Negotiations

2.1 Negotiations in the course of a market transaction

For all types of business, markets and marketplaces provide information to the trading partners, enable establishing of binding agreements and execution of the agreed [8]. Traditional and electronic markets show various similarities. Conceptually an electronic market is an application based on electronic communication services that supports the market coordination of economic activities. It is an inter-organizational application system and supports at least one phase of a market transaction. In those virtual markets, market partners can perform either parts of transactions or complete transactions electronically. The full cycle of a market transaction can be best described with a model including the following phases [9] as depicted in figure 1:

Information phase, where the relevant information concerning products, market partners etc. is gathered

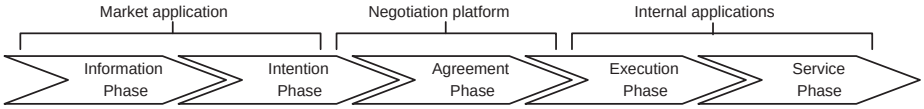

Fig. 1. Roles of the applications during a transaction

Intention phase, where offers concerning supply and demand are submitted by the market partners

Agreement phase, where the terms and conditions of the transaction are specified and the contract is closed

Execution phase, where the agreed-upon contract is operationally executed

Service phase, where support, maintenance and customer services etc. are delivered.

A negotiation can be defined as a decision-making process by at least two parties. It is performed until an agreement is reached or the process is terminated without reaching an agreement by one or all the partners involved. Its basis is the interactive exchange of information in form of issuing and adjusting offers back and forth to specify the contract particulars. Usually the objective of this process is to reach consent and establish a legally binding contract between the parties concerned, which defines all agreed-upon terms and conditions next to regulations in case of failure of their fulfillment as well as any further possible details [9]. The number of parties involved in this process and its temporal and logical conditions varies depending on the type of negotiation taking place. It may be initiated between the trading partners directly or through the intermediation of an electronic market place, which is one out of several possible realizations of electronic markets in general.

During an electronic market transaction an ad-hoc information chain is formed between the market partners. This information chain may be looked at as a temporary network, that is built dynamically and lasts until the transaction is terminated [10, 11]. Within such a dynamic business web, the applications supporting the information and intention phases can be hosted by an electronic marketplace. Components concerning the execution and service phases can be found with the partners' internal (ERP-) applications. The processes during the agreement phase are handled by an independent application. This application is the decentralized integration point, where all data services are dynamically joined together (figure 1).

2.2 An Application Architecture for Multi-Attributive Negotiations

In the MultiNeg Project [12] an electronic negotiation support system for bilateral, multi-attributive negotiations has been developed. The key objectives for the development have been the design of an architecture suitable for different industries, company sizes and products and a communication interface design that allows the integration of inter-organizational with intra-organizational applications. The functionalities are conceptualized for usage in a decentralized deployment and are based on open standards. Thus they allow the seamless electronic integration of internal and external business processes.

The architecture has three application layers, which are the Business Object Framework

Layer providing the metastructure for negotiating, the Negotiation Layer and the Communication Layer. Each layer is represented by a major component in the application architecture (figure 2):

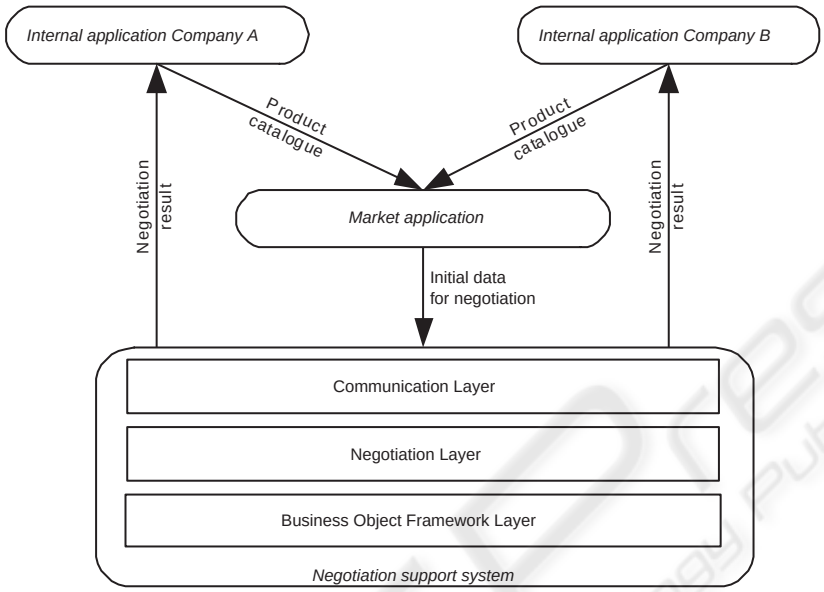

Fig. 2. MultiNeg Architecture

Business Object Framework Layer supports the management of the application's business object framework containing the specific object and document structures.

Negotiation Layer supports the process flow of interactive, bilateral multi-attribute electronic negotiations.

Communication Layer supplies the communication functions required by the other two layers. It handles incoming and outgoing messages and provides authentication and encryption functionality. It also supplies workflow functionality to manage the negotiation process flow with internal or external, human or electronic agents.

3 Security Aspects and Requirements

Due to its availability and flexibility, the Internet is used as the communication platform for dynamic business webs as described above. However, this design decision has undesirable side-effects, since the Internet is an open and anonymous network, security issues can arise. These issues can be attacks such as masquerading, or spying out confidential data etc. These threats strike at the very foundation of all transactions, which is trust. Trust is of vital importance for all communities, since it builds the basis for any kind of interaction [13]. Non-existence of any security measures leads to a lack of trust which will significantly impede the widespread acceptance of any e-business application. Therefore we introduce security services for the given dynamic business web:

Authentication: In general authentication can be classified according to the purpose desired. Either mechanisms to prove or verify the authenticity of a claimed identity (entity authentication) or the authenticity of a message (message origin authentication) are needed. In the following our understanding of authentication will always be in the sense of entity authentication. The aspect of authentication is crucial in dynamic business webs, since they tend to involve much less stable business relationships. Business partners do not necessarily know each other before starting business conduction. Therefore they need reliable authentication services to build up trust, which is key to concluding business transactions.

Authorization: This means the granting of rights, which includes access based on access rights. For instance, the access to product inventories of the parties involved in a negotiation within the application should be controlled.

Data confidentiality: All messages exchanged between business partners in the course of transaction should be private. It should not be possible for an unauthorized third party to eavesdrop on negotiation details.

Non-repudiation: The purpose of the non-repudiation service is to provide evidence of a particular event or action. Non-repudiation is essential for e-business applications. Without it business partners can later deny any involvement in concluded negotiations.

In this paper we address authentication and authorization services and develop an identity management framework.

4 Communication Services

To enable full electronic business conduction the applications used by all parties involved in an electronic transaction need to be coupled. The internal systems and applications such as ERP-systems of buyer, seller, electronic marketplace and negotiation system can form an integrated, but still flexible information chain. Consequently in MultiNeg we developed several web services in order to build up information chains in an flexible manner.

4.1 Description of the Services

The developed service components may be coupled with electronic marketplaces, but may also be used stand-alone. They can provide a faster process flow and at the same time also increase the quality of the exchanged information. To achieve this goal the close integration of the negotiation system into the information chain coming into being is mandatory. For designing such communication services the security aspects as described above need to be taken into account besides the consideration of handling the variety of existing syntaxes and semantics.

By combining web service technology with the principles of decentralized, distributed processing, the application components can be dynamically coupled each time individually precisely as needed for performing all business transactions possible. Within the so created information chain transactions can be executed by application components

especially combined for each phase. The components are distributed among the parties involved. Figure 3 depicts the overall architecture of an evolving dynamic business web. A certification authority (CA) has to guarantee the authenticity of public keys within the

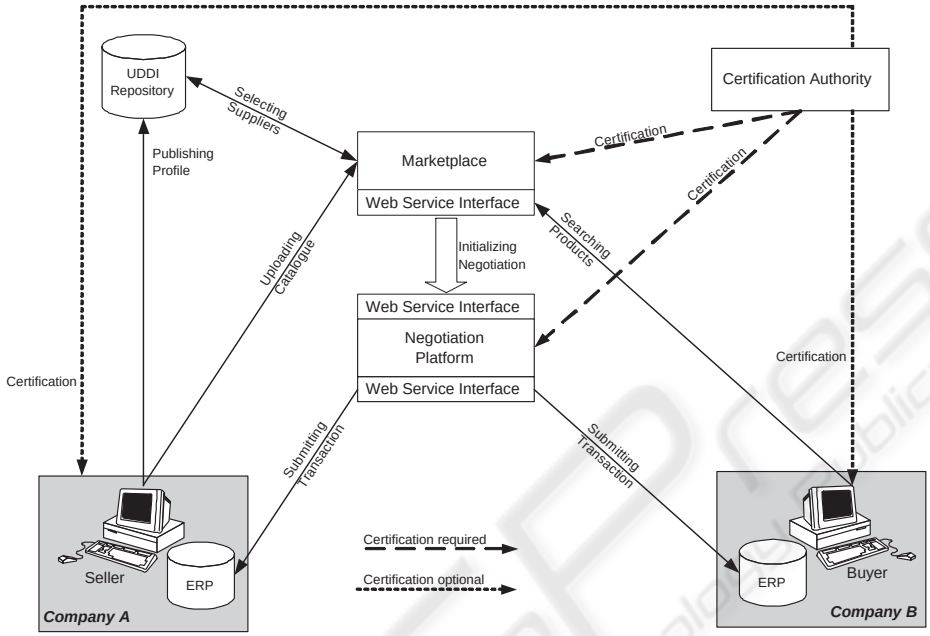

Fig. 3. Dynamic Business Web

presented scenario. For this purpose it issues digital certificates for business partners, the marketplace and the negotiation system. These certificates are trusted by all parties concerned. Possessing a digital certificate is optional for business partners. However, not to have a certificate may cause implications regarding business processes. These implications will be detailed later.

Business transactions are initialized on the electronic marketplace and are transferred to the independent negotiation system through web service interfaces. Within the project various web services have been conceptually developed and prototypes are operational for the integration of an electronic market in general, the negotiation system and the internal systems of the partners.

These web services enable a consistent, syntactic and semantic inter-operational data exchange from the initialization of the negotiation to the frequent information update until the final transmission of the signed contract document. The services are [9]:

Init Negotiation Service: It transfers the data for the initializing of a negotiation to the negotiation application.

Inventory Visibility Service: Through this service product descriptions can be enhanced with up-to-date inventory stock information.

Tunnel Inventory Visibility Service: This tunnel service has two functions in the integration scenario. It communicates with the inventory visibility service of the supplier via the marketplace. At the same time it aggregates the inventory stock data for

transmission to the negotiation system. Assuming several suppliers offering such inventory services, this visibility service is able to combine the web services of all suppliers aggregated into one front-end information.

Catalogue Update Service: This service provides the updating process of a catalogue. Using the product identification numbers the marketplace's backend generates an up-to-date catalogue extract and transmits it to the negotiation systems.

Contract Transmission Service: The transaction information of a successfully concluded negotiation is supplied by the negotiation system to the partner's internal systems through this service.

4.2 Identity Management

The core task of identity management is to answer the question "who can do what when". This simple question depicts the two core tasks of identity management, namely authentication and authorization.

Due to the lack of physical contact in online environments, such as dynamic business webs as described above, there exists an inherent uncertainty which may hamper business transactions. One sound approach to overcome this shortcoming would be the introduction of an intermediary. An intermediary is a third party who facilitates a deal between two other parties by providing certain services. There are good reasons for having intermediaries, c.f. [14]. For instance, intermediaries may offer value added services, such as aggregation, matching, facilitation, and also trust establishment. The latter service is often carried out by a so-called "trusted third party". The term trusted third party is used to describe a security authority or its agent, trusted by other entities with respect to security-related activities. Since business partners have to trust the marketplace, the marketplace itself is a perfect candidate for acting as a trusted third party offering authentication services.

The first step is the authentication process[15]. In our scenario the marketplace supports two authentication mechanisms:

weak authentication schema, such as Login/Passwords. The reason for supporting weak authentication schemes is to lower the barrier for entering the marketplace.

strong authentication schema, such as challenge-response identification based on digital certificates. By doing so the marketplace asserts the validity of the certificated issued by the CA.

Both authentication schemes can be realized using the Transport Layer Security technologies(TLS/SSL), which is the only current ubiquitous cryptographic infrastructure [16]. In our scenario server, i.e. the marketplace, authentication is compulsory, whereas client, i.e. company A, authentication is required only in case of strong authentication needs.

After a successful authentication the marketplace issues an assertion for company A. An assertion conveys information about authentication acts performed by different parties. The assertions in our scenario are issued by the marketplace and contain detailed information about the authentication process, e.g. time and schema. Furthermore they are digitally signed by their issuer.

Company A can use the assertion to prove its identity to company B. The latter has two options to verify the integrity and the authenticity of the assertion. It can verify the attached signature itself or forward the assertion to the issuer, who is here the marketplace. The choice between these options may depend on the specific circumstances of a particular business scenario.
In contrast to authentication services, authorization services have to be decentralized, since each (business) party is the only one able to grant access to its own resources. As a consequence, there is no single policy decision point. We detail a possible authorization scenario with help of examples. We focus on the Init Negotiation Service and the Tunnel Inventory Visibility Service.
For sake of better comprehensibility, we assume that company A is interested in negotiating for products offered by company B. The Init Negotiation Service runs on the marketplace and uses the web service interface of the negotiation system to transfer all data necessary for a negotiation. It includes the catalogue data as well as the assertion of company A. The assertion has been issued by the marketplace during the authentication phase, thus it enables company B to find out more about the identity of company A. As described before, the negotiation system can be customized by its users. Companies can exploit this functionality even further and may derive negotiation strategies from assertions. Company A could perhaps define different classes of negotiation partners. The specific class depends on both the authentication schema stated in the assertion and the experiences gained in past negotiations. Consequently, the class of a business partner reflects the level of trust extended towards that partner. It may influence specific negotiation settings like payment conditions or special price offers. In case company B just uses login/password to authenticate itself towards the marketplace, company A could have defined the policy of not accepting payment by invoice after delivery.
The Tunnel Inventory Visibility Service described above offers authorization in addition to aggregation and anonymity services. This is achieved through setting up policy decision points in order to define access rules for different negotiation partners or types of partners.
Again we consider the scenario where company A and company B are involved in a negotiation. We assume that company B wants to add some new items into the ongoing negotiation. For this purpose it makes use of the Tunnel Inventory Visibility Service, which expects to get company B's assertion. Access to sensitive information, such as price and availability of goods, can be controlled on the basis of that assertion. For example, in consequence company A could set up individual catalogues for its business partners.

5 Related work

Research in the field of support for electronic negotiations concentrates around the implementation of negotiations protocols [5, 17], application of agents [18, 19] or the communication flow [20]. Even though the need for security has been part of recent conceptual design discussions [21, 22], present designs require enhancements for the provision of user authentication beyond password control [21, 23] in order to grant successful implementation of an identity management concept.

There has been some remarkable industrial effort in the field of identity management aiming at developing standards for single sign-on mechanisms for the Internet. The most known among them is Liberty Alliance [24]. Although the architecture developed by Liberty Alliance is sophisticated, it is not suitable for B2B scenarios, since it mainly focuses on providing single sign-on mechanisms [25] for B2C scenarios.

6 Conclusion

In this paper we presented a web-based system, offering different services for enabling electronic negotiations for business partners. Our approach is integrative and flexible due to its modularity. Each component can be used either stand-alone or in conjunction with other components. In order to increase the creation of dynamic business webs, it offers both the possibility to use standard services and the possibility to customize them. These possibilities allow business partners to adjust parameters according to specific needs. Especially flexible are the security services, where involved parties can decide themselves how much security they need. Within the security context we focused on identity management for different services. For that purpose we developed an approach which is centralized regarding authentication and decentralized concerning authorization. Business partners want to rely on existing authentication services offered by a trustworthy party, which could be a marketplace. In our approach we support different authentication schemes. Selection and acceptance of the proper authentication schema is up to the business partners. For authorization, which is based on authentication, we concluded that only a decentralized solution can meet the needs of business partners. They are responsible for setting up access control rules themselves. For that purpose respective the services are configurable by their users.

References

1. Schönherr, M., Gallas, B.: Komponentenbasiertes EAI-Framework unter Einsatz und Erweiterung von Web Services. In Uhr, W., Esswein, W., Schoop, W., eds.: Wirtschaftsinformatik 2003 / Band II, Medien, Märkte, Mobilität. Physica-Verlag (2003) 125–142
2. Schubert, P.: E-Business-Integration. In Schubert, P., Wölfle, R., Dettling, W., eds.: E-Business-Integration, Fallstudien zur Optimierung elektronischer Geschäftsprozesse. Hanser (2003) 1–22
3. Rebstock, M., Thun, P., Tafreschi, O.: Supporting Interactive Multi-Attribute Electronic Negotiations with ebXML. Group Decision and Negotiation **12** (2003) 269–286
4. Bichler, M.: The Future of eMarkets - Multi-Dimensional Market Mechanisms. 1 edn. Cambrige University Press (2001)
5. G. Kersten and K. Pong Law and S. E. Strecker: A Software Platform for Multiprotocol e-Negotiations. http://interneg.concordia.ca/interneg/research/papers/2004/04.pdf (2004)
6. Merz, M.: E-Commerce und E-Business - Marktmodelle, Anwendungen und Technologien. dpunkt Verlag (2002)
7. Rebstock, M., Tafreschi, O.: Secure Interactive Electronic Negotiations in Business-to-Business Marketplaces. In Wrycza, Stanislaw, eds.: Proceedings of the Xth European Conference on Information Systems (ECIS2002). (2002) 564–572
8. Schmid, B.: Elektronische Märkte - Merkmale, Organisation und Potentiale. In: Management-Handbuch Electronic Commerce. 1 edn. Vahlen (1999) 31–48

9. Rebstock, M., Lipp, M.: Web Services zur Integration interaktiver elektronischer Verhandlungen in elektronische Marktplätze. Wirtschaftsinformatik (2003) 293–306
10. Cachero, C., Gomez, J., Parraga, A.: Extending UML for the migration of Legacy Systems to the Web. VI Jornadas de Ingeniería del Software y Bases de Datos (2001)
11. Cachero, C., Gomez, J.: Conceptual navigation analysis: a device and platform independent navigation specification. In: 2nd Int. Workshop on Web Oriented Software Technology. (2002)
12. MultiNeg Consortium: MultiNeg Project. http://www.fbw.fh-darmstadt.de/multineg (2005)
13. Abdul-Rahman, A., Hailes, S.: Supporting Trust in Virtual Communities. In: HICSS '00: Proceedings of the 33rd Hawaii Int. Conference on System Sciences-Volume 6, IEEE Computer Society (2000)
14. Bailey, J., Bakos, Y.: An Exploaratory Study of the Emerging Role of Electronic Intermediaries. Int. Journal of Electronic Commerce **1** (1997)
15. Menezes, A.J., Oorschot, P., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press series on discrete mathematics and its applications. CRC Press (1997)
16. T. Dierks, C.A.: The TLS protocol version 1.0 RFC 2246, IETF (1999)
17. Bichler, M., Kersten, G., Strecker, S.: Towards a Structured Design of Electronic Negotiations. Group Decision and Negotiation **12** (2003) 311–335
18. Zarnekow, R.: Softwareagenten und elektronische Kaufprozesse - Referenzmodelle zur Integration. 1 edn. Gabler (1999)
19. Veit, D.: Matchmaking in Electronic Markets. 1 edn. Srpinger Verlag (2003)
20. Schoop, M., Jertila, A.: Electronic Commerce in the Semantic Web Era. In M. Bichler and C. Holtmann and S. Kirn and J. P. Müller and C. Weinhardt, ed.: Coordination and Agent Technology in Value Networks,Multikonferenz Wirtschaftsinformatik (MKWI 04). (2004)
21. Yuan, Y., Turel, O.: A Business Model for e-Negotiation in Electronic Commerce. http://www.kluweronline.com/issn/0926-2644/ (2005)
22. Neumann, D., Benyoucef, M., Bassil, S., Vachon, J.: Applying the Montreal Taxonomy to State of the Art E-Negotiation Systems. Group Decision and Negotiation 12 (2003) 287–310
23. Ye, S., Makedon, F., Steinberg, T., Shen, L., Ford, J., Wang, Y., Zhao, Y.: SCENS: a System for the Mediated Sharing of Sensitive Data. In: Proceedings of the 3rd ACM/IEEE-CS joint conference on Digital Libraries. (2003)
24. Project, L.A.: Liberty Alliance Specifications. http://www.projectliberty.org/resources/specifications.php (2005)
25. J. De Clercq: Single Sign-On Architectures. In Davida, G.I., Frankel, Y., Rees, O., eds.: Proceedings of Infrastructure Security, InfraSec. Number 2437 in LNCS, Springer (2002) 40–58